 DOI: *https://doij.org/10.10000/IJLMH.118445*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 6

2024

Search and Seizure Powers of the Police under the Cybercrimes Act 2015: Lesson From South Africa Best Practice

TUKUSWIGA IKASU[1]

ABSTRACT

The celebrations for communication technological advancement did not come empty-handed. On the one hand, it brought developments in the computerized communications that have guaranteed effectiveness and efficiency in that arena. On the other hand, cybercrimes have become a daily menu in the criminal justice plate. In fighting against new criminality, Tanzania enacted the Cybercrime Act in 2015. In the process of investigating such crimes, Part IV of the Act empowers the police to conduct search and seizure. With all the appreciations for the good work of the Legislature in enacting this law, it has been vividly observed that the Police wield uncontrolled and discretionary powers in that respect. The Cybercrime Act has several weaknesses such as vesting wide and inflated discretionary search and seizure powers on the police and limiting the court involvement in the process. To remedy the weaknesses, ken eye has to be opened to the countries with best practice in this area. The article does a comparative discussion between the Tanzania Cybercrime Act, 2015 with South Africa Cybercrime Act, 2020 so as to formulate some recommendations on how Tanzania can amend, rectify and improve police powers of search and seizure during computer and cybercrime investigations.

Keywords*: search, seizure, police powers, cybercrime, cybercrime investigation, computer data, computer system, computer devices, electronic evidence, warrant.*

I. INTRODUCTION

Cybercrime refers to a criminal activity committed using or against a computer, a computer system, network, or digital devices.[2] It also means crimes committed in the cyberspace. Cybercrime is also called computer crime as it involves the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy.[3] According to the United States of America Department of Justice, computer or computer system involvement can be in three

[1] Author is a LL.M. Student at University of Iringa, Tanzania.

[2] Brush K and Cobb M, 'Cybercrime'<www.techtarget.com/searchsecurity/definition/cybercrime> accessed 31 January 2024.

[3] Ibid.

 [ISSN 2581-5369]

categories; as a weapon for a crime commission, as a target of the crime and as an accessory to its commission.[4]

(A) Search and seizure

Search and seizure are some of the procedures in cybercrimes investigation. On the one hand, search is an act whereby the law enforcement officer conducts an examination into a person's property such as house, vehicle, computer devices, business, etc. with the intention of finding evidence for the crime suspected.[5] On the other hand, seizure is the result of search which consists in the act of taking possession of the searched property for further investigations.[6] SADC Model Law uses the terms search and access interchangeably. Access is simply defined as entering a computer system.[7] The term seize is also used interchangeably with secure to mean activating onsite computer system and computer data storage media; making and retaining a copy of computer data, maintaining the integrity of the relevant stored computer data, rendering inaccessible, or removing, computer data in the accessed computer system; taking a printout of output of computer data; or seize or similarly secure a computer system or part of it or a computer data storage medium.[8]

(B) Cyber data

The term "cyber data" is synonymous to computer data, digital data or electronic data; hence the definition of one stands for all. Computer data is defined as, 'any representation of facts, information or concepts in a form suitable for processing on a computer system, including one suitable to cause a computer system to perform a function.'[9]The Tanzania Cybercrime Act defines computer data to mean any representation of facts, information, concepts or instructions in a form process able in a computer system.[10]This representation of facts, information, concept or instructions should be the organized and meaningful end product of data processing for it to be admissible evidence in a court of law.[11]

When police are conducting cybercrime search and seizure, the target is to access the cyber data **so** as to collect electronic evidence for further investigation.

---

[4]Ibid.
Legal and Information Institute, 'Search and Seizure' <www.law.cornell.edu/wex/search_and_seizure> accessed 8 April 2023.
[6]Ibid
[7]SADC Model Law on Computer Crime and Cybercrime 2022, art 3
[8]Ibid.
[9]European Council Convention on Cybercrime 2001, art1 (b).
[10]Cybercrime Act 2015, s 3.
[11] Vinesh Basdeo, Moses Montesh and Bernard Lekubu, 'Cyber Environments: A Law-Enforcement Dilemma in South African Criminal Procedure' 1(1) Journal of Law, Society and Development 2014, 48 p 50 < https://unisapressjournals.co.za/index.php/JLSD/article/view/874> accessed 23 June 202450.

 [ISSN 2581-5369]

(C) Electronic evidence

The target of search and seizure in cybercrime is to collect electronic evidence to be admitted in court. Thus, electronic or digital evidence may simply be defined as information that is stored or transmitted electronically and which can be used in a court.[12] Electronic information from the computer is of two categories. The first category includes that information that the computer itself generates. These are data that have not been created by the computer user.[13]They are simply referred as computer self-generated information and they include but not limited to operating systems, databases, programs, automated telephone call records. Another category is the category of computer stored information. These are the electronic information that has not been generated by the computer but by the user. The user can command the existence or non-existence of that information. They are regarded as computer stored data as they are only stored but not self-created by the computer. Data such as photos, electronic messages, voice mail, and chart are regarded as computer stored information. [14]

Electronic information can be stored in different computer storage devices such as hard drives, memory cards, Central Processing Unit (CPU), mobile phone, floppy disk and Compact Disk.[15]

In spite that electronic data has taken dominance in the investigative information, collection of the same is a tedious task. This is due to the fact that this kind of evidence has unique characteristics compared to the physical evidence in traditional criminal investigation. Handling electronic data is a complicated task due to the several reasons. One of the main reasons is that volatility and fragility of these data. Compared to physical evidence, electronic evidence can be easily tempered.[16] For instance, if evidence is in the physical file for a suspect to get rid of that file will have to burn it or throw it away. This destruction of the physical file may time some movements and time of which if the suspect is not faster enough may be caught before finishing his or her evil act. In cybercrime, if the same suspect wants to get rid of even ten electronic files he/she can do it at a click of a figure without anyone noticing what is taking place.[17]Moreover, electronic evidence requires special expertise and tools to retrieve, collect, preserve, examine for it to maintain evidential value in the court of law worthy to be admissible.[18]In regard of this,

[12]ibid.
[13]Raja Vijayaraghavan, 'Digital Forensics Collection, Preservation & Appreciation of Electronic Evidence'<https://nja.gov.in/Concluded_Programmes/2021-22/P-1271_PPTs/1.Digital%20Forensics%20Collection,%20Presservation%20and%20Appreciation%20of%20Electronic%20Evidence.pdf>accessed 9 July 2024.
[14]Ibid 11.
[15]Ibid.
[16]Vijayaraghavan (n 12) 5.
[17]Ibid.
[18]Ibid 6.

 [ISSN 2581-5369]

search and seizure in cybercrime requires the police officer to have special skills and tools to effectively search and seize digital evidence.

II. LAW GOVERNING POLICE SEARCH AND SEIZURE POWERS IN TANZANIA

The Tanzania Cybercrime Act, 2015 is the principal law in cybercrime matters in Tanzania. The Act provides for investigation, collection, and use of electronic evidence and other related matters[19]; among others. The Act has specific provisions on search and seizure found under Part IV. This part, among other things, gives the search and seizure powers to the police. Such powers are provided under section 31 (2) which provides that any authorized police officer can execute search and seizure under the order of police in charge of a police station or a law enforcement officer with similar rank. The Act empowers police to search the computer system[20], computer data[21]or computer device[22] where there is a reasonable ground to believe that the mentioned items may be used as evidence in proving a case or is acquired as result of an offence.[23]

(A) Law governing police search and seizure powers in South Africa

The procedural aspect of cybercrime in South Africa are principally governed the Cybercrime Act, 2020. The aspects of search and seizure are covered under chapter 4 of the Act. Although the Act is recent compared to the one of Tanzania, it can be observed that there are good inputs that Tanzania can adopt for better improvement of search and seizure practice.

III. A COMPARATIVE ANALYSIS OF THE PRACTICES IN TANZANIA AND SOUTH AFRICA

In the next part, the article discusses the police search and seizure powers as practiced in Tanzania in comparison with the best practice in South Africa in order to grasp the best practices that Tanzania can extract from South Africa.

(A) The requirement of a search warrant.

Going through Part IV of the Tanzania Cybercrime Act, 2015 Act there is no provision obliging the police to apply for a court warrant before execution of search and seizure. The Act has completely omitted the requirement of a court warrant in all circumstances of search and seizure. In other words, all searches and seizures under the Act are warrantless. Under the Act,

[19]Cybercrime Act 2015, preamble.
[20]Cybercrime Act 2015, s3.
[21]ibid.
[22]Encyclopaedia, 'Computing Device' <www.pcmag.com/encyclopedia/term/computing-device> accessed 10 January 2024.
[23]Cybercrime Act 2015, s 31(1)

search and seizure is initiated by the order of the police officer in charge of a police station or an officer of a similar rank.[24] This officer is vested with unchecked discretionary powers in authorizing and approving search and seizure of cyber data. This means that it is the officer who establishes the grounds for search, the one scrutinizing his own grounds, and he/she is finally the one approving his or her own decision. Under the Cybercrime Act, once the police officer in charge of the police station issues a search order then it will be executed by the police officer as ordered. The execution is straight from uncross-checked order by authorizing police officer.

This kind of discretionary power poses some risks in the criminal justice system per the analysis below.

First, it is well understood that police officers are on the prosecution side when it comes to criminal investigation. The prosecution side is the one responsible to prove the case beyond reasonable doubts by collecting enough incriminating evidence against the suspect. In this sense it is undeniable fact that if not limited, they may be too aggressive and pressured to find the evidence on the case to the point of giving the broad search orders that will victimize the person in control of the device or computer system. The fact that the Cybercrime Act has left these wide discretionary powers on the police to issue a search order and the latter to be executed without a crosscheck by the judiciary in any way, indirectly justifies a chaos in right to data privacy of citizens in the country. To avoid this chaos in South Africa[25], the law specifically requires the enforcement officer to have a court warrant prior to the execution of search and seizure. A court in South Africa court held that when the police officer fails to obtain search warrant in circumstances where it was possible to do so and there was enough time to obtain such warrant, warrantless search will be termed as illegal.[26]The rationale is to make sure that the court scrutinizes the grounds as well as the whole scope of search and seizure so as to see if the grounds are reasonable to justify search and to limit the police's powers to the desired target only.

Second, it is through the warrant that the so-called reasonable grounds by the police are crosschecked to see if they are really reasonable to justify execution of search and seizure. Logically all grounds are reasonable in the sight of the one forming them but one the third neutral party scrutinizes the grounds it may be found out that all or some of the grounds are not reasonable as they were considered to be. In the same sense, even grounds for search and seizure by the police are reasonable in their own sight and if not crosschecked by the judiciary there is

[24]Ibid
[25]Cybercrime Act 2020, s 29(1).
[26]Ngqukumba v Minister of Safety and Security 2014 (5) SA 112 (CC)

a danger of executing search and seizure basing on unreasonable grounds. Executing search and seizure basing on unreasonable grounds amounts to violation of right to privacy of persons in the country which is contrary to article 16 (1) of the Constitution of the United Republic of Tanzania.

Third, warrantless search is an exception to the general rule that requires that search and seizure operation be conducted under warrant.[27] Warrantless search should not be a general rule but only an exception to the general rule. Warrantless search is reasonably expected to be applied in some exceptional circumstances provided by the law. Such exceptional circumstances may include but not limited to; boarder search, exigent circumstances, in plain view or during lawful arrest.[28] The exceptions that justify warrantless search should be specifically established and well- delineated by the particular law.[29] Unfortunately, the Cybercrime Act does not have provisions differentiating searches and seizures under normal circumstances from those under urgent situations. The Act has the same search and seizure provisions to be applied in two opposing circumstances. Looking at the Cybercrime Act of South Africa, circumstances that the police officer may execute warrantless search have been clearly provided to include search in emergence, [30]search on arrest[31] and search on consent.[32]

On the part of South Africa, the general rule under the Cybercrime Act requires search and seizure to be conducted under the authorization of search warrant. The Constitutional Court warned that search must be done under authorization of warrant as the latter softens the intrusion to privacy as it road maps the specific scope of the search.[33] This search warrant must be issued by the magistrate or a high court judge upon the written application by the police officer.[34]The judicial officer being an independent and neutral party possesses adequate skills and abilities to scrutinize the application and make the right decision for justice sake.[35]The question as to who to search, what to seize and what extent are provided and limited by the search warrant. Reading trough the Act, there is consistent use of the phrases such as 'as identified in the search warrant'

[27] Peter Du Toit, 'The Search Warrant Provisions of The Cybercrimes Act and Their Relationship with The Criminal Procedure Act' (2022)43(4) Port Elizabeth p.765< www.scielo.org.za/scielo.php?> accessed 21 March 2023.
[28]Nathan Judish, '*Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*' (3rd edn, United States, Office of Legal Executive Office for United State Attorneys2003) 15-40 < www.justice.gov/file/442111/> accessed 21 March 2023.
[29]Donald Resseguie, 'Computer Searches and Seizure' (2000)48, Clev. St. L. Rev. 185, p.185, <https://core.ac.uk/download/pdf/301536939.pdf >accessed 16 June 2024.
[30]S 32.
[31]S 33.
[32]S 31.
[33]Gaertner v Minister of Finance 2014 (1) SA 442 (CC) 69.
[34]Cybercrime Act 2020, s 29 (1) (a).
[35]Minister for Safety and Security v Van der Merwe 2011 (2) SACR 301 (CC) 38

and 'to the extent identified in the search warrant'.[36] This is to limit the police officers to in boundaries of the search warrant. The Act leaves no discretionary powers on the police regardless of the rank to authorize or conduct search and seizure in their discretionary manner.

All searches done without search warrant under non exceptional circumstances are declared illegal by the courts. This was confirmed in *Gumede v S*[37]where the Constitutional Court declared search without warrant illegal if the police officer fails to obtain the warrant while he was not acting under urgent circumstances and that he had enough time to obtain it. The police officer executing search and seizure under a search warrant is empowered to search any kind of article as defined under section 1[38]and execute any seizure powers as provided under the definition of seizure in section 25 of the Act.

In making sure that all search and seizure are conducted under the court search warrant, the Act allows oral application for search warrant in case written application cannot be done. It is understood that in some case it may be reasonably impractical to prepare a written application before searching due to the urgency or exceptional circumstances.[39]In such kind of scenarios, the specified police officer does an oral application for search warrant.

(B) The warrantless search

The practice in Tanzania is that all search and seizures are executed without warrant. Going through part IV of the Cybercrime Act, there is no provision obliges the police officer to apply for search warrant before executing search and seizure operations. In other words, all search and seizure under the Act are warrantless.

The practice in South Africa has not turned a blind eye on the reality that in some scenarios the searches through search warrant whether written or oral applied is impossible due to some factors. In this sense, the Act allows the practice of conducting search without warrant. If the police officer has grounds to believe that a search warrant would be issued if applied but the delay of getting that warrant will defeat the object of search, the warrantless search will be valid.[40]

The powers of the police under this category are limited to some actions and articles only. The police officer searching without warrant is authorized to execute only two seizure powers provided under paragraph (a) and (b) of the definition of seizure.[41] Seizure powers under

[36]Cybercrime Act 2020, s 29 (2).
[37](800/2015) [2016] ZASCA 148.
[38]Cybercrime Act, 2020.
[39]ibid s 30.
[40]Cybercrime Act 2020.
[41]ibid s 25.

 [ISSN 2581-5369]

paragraphs (a) and (b) are powers to remove to data storage medium or any party of a computer system; and power to render inaccessible data, computer program, and computer storage medium or any part of the computer system respectively. Those two seizure powers are also limited to be executed on two categories of article defined in paragraphs (c) and (d) of the definition of the term article as provided under section 1.[42] These articles under paragraphs (c) and (d) includes computer data storage medium and computer system respectively. This kind of limit does not exist when the police officer is searching with warrant. During search with warrant, the police officer has four seizure powers which are, from paragraphs (a) - (d) to be executed on all four categories of article under paragraphs (a) – (d) of the definition of the term article.[43] Something to learn from the difference of powers of police officer when conducting search with warrant and warrantless search is that search without warrant is less trustworthy even if it is inevitable in some cases. Hence, even if it is inevitable in some scenarios, the risk to privacy intrusion by a warrantless officer should be well calculated and limited. In this regard, the South Africa law has narrowed the scope of the powers of police to search and seize in warrantless search so limit their discretionary powers to a certain extent only.

(C) The powers to issue orders.

In Tanzania, the orders of disclosure of data[44], exigent preservation of data[45], disclosure and collection of[46] traffic data or content data [47] or information are at the discretion of the police. Under the Act, the police have powers to order the person in the possession of the data in the mentioned categories to ether disclose, preserve, collect, and permit or assist the police officer to collect such data. All these orders target disclosure or preservation of data; so, the two terms will stand for other terms used (such as collection, recording, assisting police officer to collect or record data). On the one side, when ordered person collaborate as ordered then it will be executed peacefully. On the other side, when disclosure and preservation of data cannot be done without the use of force, then the police have been given discretionary powers as to whether to apply for court orders to affect the disclosure or preservation of data. This kind of power was observed in *Jamii Media Ltd v. Attorney General*[48] whereby the police issued orders compelling the Jamiiforums to disclose the Internet Protocol (IP) addresses of its anonymous users and

[42]ibid.
[43]Cybercrime Act, 2020, s 1.
[44]Cybercrime Act 2015, s 32.
[45]Ibid.
[46]ibid s 34.
[47]ibid s 35.
[48]Miscellaneous Application, No.9 of 2016, High Court of Tanzania at Dar es Salaam.

other information that would help the police to identify them.

Section 36 of the Cybercrime Act shows that the court involvement in issuing the mentioned orders is optional. This means that the police may or may not do what the Act instructs as it has been left at its discretion to decide the direction to take. The section clearly shows that the court will be consulted only if the disclosure or preservation cannot be done without the use of force. The use of the term 'may' entails that it is at the police discretion and not a mandatory one. This is risky because it is possible to have a scenario that the disclosure or preservation cannot be done without the use of force and still the police opt not to apply for a court order for that effect.

It is argued that the court should be the one issuing orders of disclosure or preservation in the first place not the police. The police should apply to court for it to issue the orders after satisfying itself with the grounds in the application. This is to limit the aggressiveness of the police to find evidence by issuing disclosure orders whenever reasonable in their own sight.

Another headache is that the Act has not specified as to which offense disclosure order should be issued. This means that any kind of cybercrime whether severe or not, may attract a disclosure or preservation orders by the police. In summary, there are two main weaknesses under this part. There is an issue of the exclusive and discretionary powers extended to the police without the court's involvement. There is an also additional discretionary power to decide whether to involve the court or not even in serious circumstance such as when disclosure or preservation cannot be done without the use of force. It would be health for the Act to compel that once a law enforcement officer cannot get disclosure or preservation of information or data without the use of force, he/she must apply for a court order. This was well cemented in *Jamii Media Ltd v. Attorney General*[49]where the High court emphasized that the police must seek the court intervention in circumstance when they fail to secure data under section 32 of the Cybercrime Act.[50]

In South Africa the powers to order preservation of evidence or disclosure of data is strictly vested in the magistrate or judge.[51] When the police officer has reasonable grounds to believe that a person, financial institution or communication service provider has some evidence to be preserved or some data to be disclosed, he/she must make an application to the court to that effect.[52] It is within the court's power to scrutinize the application and decide accordingly.

[49]Ibid.
[50]Cipesa, 'State of Internet Freedom in Africa 2018 Privacy and Personal Data Protection in Tanzania: Challenges and Trends' 2018, p.20 < https://cipesa.org/wp-content/files/reports/State-of-Internet-Freedom-in-Tanzania-2018.pdf> accessed May 16 2024.
[51]Cybercrime Act 2020, ss 42 and 43.
[52]Ibid.

 [ISSN 2581-5369]

Also, one of the factors to consider in issuing preservation order is the legitimate interests of other persons in proportion to the severity of the offence in question.[53] In other word the authority must weigh the legitimate interest in relation to how severe the crime is and then decide whether to issue an order or not. The orders are not issued blindly and in regardless.

Apart from that, there is a clear consideration of the concerns from the person to whom the direction was issued. Even though the direction is issued by the court, which is a more superior than the police, still the victim is given a chance to challenge it by way of application on ground that they cannot timeously or in a reasonable fashion, comply with the direction. Upon the application by the victim of the direction, the court may amend or even cancel the Disclosure or preservation direction.[54]

The lesson that Tanzania can learn from this part is that orders like these should be left to the court for issuance. The police should not be left with discretion to issue this kind of orders or directions. Another thing is that the victims should be given a chance to oppose the order rather than being harsh and limiting their right to be heard once not in position to comply.

(D) Proportionality to severity of the offense.

In South Africa, when searching and seizing suspected cyber articles, a victim's right to enjoy the use of computer devices, computer program and computer system is put on suspense for some period of time. Minding that those articles may be very crucial for a person to enjoy some right or fulfil some responsibilities, the Act limits the police officer executing search and seizure to have a due regard to the rights, responsibilities and legitimate interest of people in proportion to how severe is the crime. This means that the gravity or severity of the offence should be a determinant factor on seriousness of measures to be taken in weigh against severity the crime. How lenient should the search officer be in regard to the right, responsibilities and interest will be dependent on the gravity of the offence. In other words, the police should not act like robots by taking lenient or serious measures regardless of how simple or severe the crime at hand is. [55]

On this aspect, Tanzania should take in this best legal practice by specifically having the provision in the Cybercrime Act on that aspect. As it is currently, the police conduct search and seizure in all cybercrime investigations applying same level of measures regardless the gravity of the offense. The Cybercrime Act, 2015 leave the discretion on the police to decide the gravity

[53]Ibid s 41 (1).
[54]Cybercrime Act 2020, ss 42 (5) and 44 (5).
[55]Cybercrime Act 2020, s 36 (b).

 [ISSN 2581-5369]

of the measure to be taken in the course of search and seizure. In other words they may take serious measures of search and seizure in a simple crime or verse versus.

(E) The Standard Operating Procedures.

The South Africa under section 26 of the Cybercrime Act, 2020[56] establishes the SOPs for the investigation, search, access or seizure of articles. They provide a uniform standard to be observed by any South Africa Police Service (SAPS) and anyone authorized in term of other laws.

The SOPs apart from standardizing the procedures to be observed by the searching officer, it also provides some elaboration and emphasis that if not provided then the procedure of search and seizure could vary from one officer to the other or from one case to another. Hereunder are some more elaborations on provisions of the Act that add more clear understanding on the police officer in search and seizure operations.

Under Procedure 4.1.4,[57] the police officers are reminded to remember the order of the definition of the term "article" as stated in the Act[58] because only certain categories of articles can be searched and limited seizure actions only can be executed when searching without warrant. Under procedure 13.4.1, the SOPs explains that just like in 'Layby Principle', the police acting under warrantless search can seize computer data storage medium and computer system. Upon seizure, the police officer can only execute two seizure powers under paragraphs (c) and (d). If the police desire to execute all the seizure powers in paragraphs (a) to (d) he/she must fulfil the procedure and acquire a search warrant in term of section 29 of the Cybercrime Act.

The SOPs also answer the question concerning which article to be seized and evidence to be collected at the crime scene.[59]This has proved to be a complicated and difficult to figure out. In sorting the puzzle, the SOPs guide the police officer to have a proper planning by first ascertaining the type of authorization used in that case such as search warrant, warrantless search or search under lawful consent.[60]

In relation to warrant, the SOPs clearly tell what should be contained in the warrant on top of those specified under section 29 of the Act. It states that the warrant should contain cyber article, location, type of action to be taken and reference to password. By doing this, the police officers

[56]No 19 of 2020.
[57]Standard Operating Procedures 2024.
[58]Cybercrime Act 2020, s 1
[59]Standard Operating Procedures, pr 7.19.
[60]ibid pr 7.1.10.

 [ISSN 2581-5369]

will have the same format of the contents when applying for and executing search warrant.[61]Additionally the SOPs provide a limit that the reason and extent of any action during investigation procedure must be done within the ambit of search warrant.[62]

Moreover, the police officers are guided on which factors to consider when planning and preparing for search and seizure. A range of factors to be considered include but not limited to prevailing circumstance, purpose of search, nature of the article, location of the article and logistical aspect. [63]If every police officer observes these specific considerations, the conduct of search and seizure will be more effective in achieving the targeted goal.

IV. CONCLUSION

The powers under part IV have revealed some weaknesses which can be categorized into two mains themes which are wide discretionary powers of the police and the lack of court oversight in search and seizure procedure.

These weaknesses can be remedied if Tanzania considers and adopt the lessons from other countries which have the best practices in the search and seizure area. The Literature from counties such as South Africa should be consulted to extract best lessons that Tanzania can learn from.

V. RECOMMENDATIONS

The amendment of the Act specifically under Part IV is expected to yield the best version of search and seizure powers of the police in Tanzania. The suggested amendment of the Tanzania Cybercrime Act should absorb the following recommendations;

1. Search and seizure must be executed through court warrants.

The authorization of search and seizure should be conducted through court warrant unless for the exceptional circumstance specified in the Act. This will guarantee that the grounds, the scope and the mode of execution of search and seizure are well scrutinized and approved by the court. Also, all other orders such as preservation and disclosure must be mandated to be issued by the court. Before undertaking any procedure, the police must apply to the court for warrants and orders upon proving reasonable grounds. The Police should not be the one issuing and executing its own orders of search and seizure. This is to avoid unjustifiable intrusion into the right to privacy of individual in the country.

[61]ibid pr 9.6.1.2.
[62]ibid pr 11.2.
[63]ibid pr 7.4.

2. The preservation and disclosure orders should be issued by the court.

Second, all discretionary powers of the police in regard to search and seizure under Part IV should clearly be limited. The powers of the police to order preservation and disclosure of data should be removed and vested in the court. The police must always apply to the court for the orders. Therefore, discretionary powers provided under sections 32, 33(2) and 36 should be limited by replacing the word 'may' with 'shall' or 'must.'

3. The decision of the police should be subjected to challenge.

Additionally, the Cybercrime Act must offer a victim or a suspect of the search the right to challenge decisions and orders when there are reasonable grounds to do so. The Act should not close a room for the right to access the court to challenge the decision or orders affecting the victims when there are reasonable grounds. For instance, a controller of a computer system which has been removed or made accessible as part of search and seizure procedure when his or her request for accessing or copying the data has been rejected, the law should make a room for the victim to challenge the decision.[64] In line with that, preservation and disclosure orders[65] should be subjected to challenge by the victim when there are reasonable grounds for such action.

4. The establishment of SOPs under the Cybercrime Act, 2015.

Moreover, the Cybercrime Act under Part IV should establish the SOPs to makes sure that there is a uniform standard of the application and execution of search and seizure in the country. Through the SOPs, search and seizure provisions will be digested for a practical and specific execution of Part IV of the Act. This is to avoid the variation in the execution of search and seizure procedures under the Act with general provisions with no standardized procedures guiding the police.

*****

[64]Cybercrime Act 2015, s 31 (5).
[65]ibid ss 32 and 33.

 [ISSN 2581-5369]

VI. REFERENCES

- Nathan J., Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (3rd edn, Office of Legal Education Executive Office for United States Attorneys 2009)
- Basdeo V, Montesh M, Lekubu B, 'Cyber Environments: A Law-Enforcement Dilemma in South African Criminal Procedure' (2014) 1(1) *Journal of Law, Society and Development*.
- Melody M, 'Is Cyber Search and Seizure under the Cybercrimes and Cyber Security Bill Consistent with the Protection of Personal Information Act?' (2016)37 (3) *EJC*
- Nieman A, 'Cyberforensics: Bridging the Law/Technology Divide' (2009) 2009(1) *Journal of Information, Law & Technology*
- Pieter T, 'The Search Warrant Provisions of the Cybercrimes Act and their Relationship with the Criminal Procedure Act' (2022)3(4) Port Elizabeth 764
- Police Service Force, 'Standard Operating Procedures'
- www.saps.gov.za/resource_centre/notices/downloads/SAPS-CCA-SOP-FINAL-12-09-2023.pdf (accessed 7 January 2024)
- United Nation Office on Drugs and Crime, 'FAQ - New United Nations Convention
- OnCybercrime'<www.unodc.org/documents/Cybercrime/AdHocCommittee/FAQ_Jan 2022.pdf> (accessed 10 June 2024)
- Cipesa, 'State of Internet Freedom in Africa 2018 Privacy and Personal Data Protection in Tanzania: Challenges and Trends', available at < https://cipesa.org/wp-content/files/reports/State-of-Internet-Freedom-in-Tanzania-2018.pdf>, (accessed16 May 2024)
- Jamii Media Ltd v. Attorney General Miscellaneous Application, No.9 of 2016, High Court of Tanzania at Dar es Salaam
- Ngqukumba v Minister of Safety and Security 2014 (5) SA 112 (CC)
- Gaertner v Minister of Finance 2014 (1) SA 442 (CC) 69.
- *Gumede v S* (800/2015) [2016] ZASCA 148.
- Minister for Safety and Security v Van der Merwe 2011 (2) SACR 301 (CC) 38

*****

 [ISSN 2581-5369]